社交网络中关联隐私的价值计量与分析*

■ 臧国全[1,2] 周晓倩[1]
[1] 郑州大学信息管理学院 郑州 450001 [2] 郑州大学数据科学研究所 郑州 450001

摘 要:[目的/意义]伴随着社交网络的流行,用户通过社交平台大量下载使用第三方应用程序(即社交 APP),由此产生隐私关注。关注对象除个人隐私外,还包括用户朋友的隐私,即关联隐私。通过对关联隐私价值的计量,证实关联隐私的广泛存在,为社交 APP 中关联隐私政策的制定提供依据。[方法/过程]通过实证调查及文献回顾,证实关联隐私的广泛存在,提出相应研究问题及研究假设。采用联合分析法,通过问卷调查分析个体偏好,推理用户选择 APP 的影响因素,定量估计关联隐私的价值。[结果/结论]研究结果发现,用户选择使用 APP 时会考虑朋友隐私,但对朋友隐私的估值相对较低。当考虑到社交 APP 采集用户信息的情境对关联隐私价值的影响时,通过引入两种情境,即 APP 采集的用户朋友信息是否会提升 APP 的功能实现和使用效果,结果表明只有当这两种情境作用于朋友的完整信息时产生的关联隐私差异才具有显著性,这说明对用户来说,保护朋友的基本信息不是那么重要,但对于敏感信息(完整信息中去除基本信息的部分)的不合理请求会对 APP 评价产生负面效用。
关键词:社交网络 关联隐私 隐私价值 隐私计量
分类号:G251
DOI:10.13266/j.issn.0252-3116.2020.14.009

1 问题提出

社交网络的流行导致其功能不断扩展,其中之一是第三方程序(即社交 APP)的植入。用户通过社交平台下载使用这些 APP,满足各自需求。该类 APP 在市场上取得巨大成功,据统计[1],2019 年全球整体下载量已经突破 2 040 亿次,其中中国市场的下载量占到了近 50%,成为应用量最大的国家。但是,社交 APP 广受欢迎的同时,会产生用户的隐私关注问题。一方面,这类 APP 常设置有采集用户本人信息的前置条件,只有获得用户授权才可使用,但用户无法判断采集是否过度,存在被动诱导过度授权的嫌疑,也很少知晓被采集信息的详细用途,存在滥用的疑虑。另一方面,这类 APP 也常同时设置有采集用户朋友信息的许可门槛,也只有用户许可后方可使用,但无需用户朋友的同意,甚至用户朋友根本无从知晓。上述第一类关注的对象是用户自己的隐私,可被称为直接隐私。第二类关注的对象是用户朋友的隐私,即用户做出许可决定时对其朋友信息的隐私性和隐私程度的认知,这种隐私被称为关联隐私。

社交 APP 中关联隐私的存在较为普遍。一方面,社交 APP 可以请求的用户朋友信息较广泛,包括生日、照片、证件、住址、工作经历、教育背景和位置数据等,对于这类信息的采集,国内多以打包方式捆绑在 APP 用户隐私政策中告知,国外多以列表方式展现供用户选择。另一方面,社交 APP 的安装频率较高,即使其中一些 APP 只要求采集特定类型信息,作为一类应用程序的社交 APP 采集的用户好友信息也相当可观。国内方面,这类 APP 均明确采集用户的多种类型信息,但其中一些类型涉及用户朋友信息,比如用户通讯录,依据设置和用户编辑,可能包含朋友姓名、朋友电话号码、朋友住址、朋友邮箱等;用户通话记录,不仅内含用户的通话内容,也包括用户朋友的通话内容;拨打电话和接听电话,同样记载朋友电话号码,等等。因此,这类 APP 是以隐含方式采集用户的朋友信息,并且均以打包形式捆绑在隐私政策中。据中国互联网信息办公室[2]在 2019 年 5 月对安卓操作系统中 100 款常用 App 申请收集使用个人信息权限情况的调查,内

* 本文系国家自然科学基金项目"数字保存的风险型元数据与风险监控研究"(项目编号:71673255)研究成果之一。
作者简介:臧国全(ORCID:0000-0002-9606-6455),教授,博士,博士生导师;周晓倩(ORCID:0000-0003-3542-4455),硕士研究生,通讯作者,E-mail:827255891@qq.com。
收稿日期:2020-02-15 修回日期:2020-04-03 本文起止页码:85-93 本文责任编辑:王传清

含采集用户朋友的主要信息统计如表 1 所示：

表 1 百款 APP 中采集涉嫌用户朋友主要信息统计（N＝100）

采集涉嫌朋友信息的类型	采集 APP 的个数	采集 APP 的占比（%）
用户通讯录中的朋友信息	70	70
用户通话记录中的朋友通话内容	9	9
用户拨打和接听电话中的朋友电话号码	34	34
用户接收短信彩信中的朋友来信	21	21
用户手机存储器中拍摄的朋友照片	98	98

国外方面，作者在 2019 年暑期在美国学术交流期间，调查 Facebook 中 2018 年度下载频率最高的 1 500 款 APP，统计每款 APP 需用户许可访问其朋友信息的类型，汇总采集各主要类型信息的 APP 数量及占比，并依据每款 APP 在 2018 年度下载次数，计算每类信息该年度被采集次数，如表 2 所示：

表 2 Facebook 最流行 APP 采集用户朋友主要信息统计（N＝1 500）

朋友信息的类型	采集 APP 的个数	采集 APP 的占比（%）	2018 年被采集次数（万次）
照片/视频/音频	114	7.6	253.21
生日	97	6.5	151.67
住址	55	3.7	131.98
出生地	61	4.1	101.11
工作经历	86	5.7	93.09
教育背景	48	3.2	71.59
个人兴趣爱好	39	2.6	70.69
位置信息	74	4.9	70.21

基于表 1 可知，国内方面，缺乏 2019 年安卓 APP 下载次数的官方乃至民间统计数据，故无法计算各类信息被采集次数，但安卓 APP 涉嫌采集用户朋友信息现象非常普遍。基于表 2 可知，国外方面，针对其中一种类型信息，虽然采集的 APP 占比不高，但这些 APP 的被下载频率非常高，采集信息总量甚为可观。因此，无论是国内还是国外，社交网络中均存在较为严重的关联隐私现象。

关联隐私产生的理论基础是"涉他偏好"，即人们的行为决策不仅考虑自己的利益，还关注他人的利益，社交 APP 情境中，该理论意味着当用户做出下载使用涉及收集朋友信息的 APP 决策时，会考虑其朋友的利益，会关注其朋友的隐私。关联隐私价值的计量遵从情境依赖理论，即数据请求的情境相关性影响用户的信息披露行为和隐私感知，社交 APP 情境中，比如用户安装一个生日 APP 用于提醒其朋友生日，与该 APP 采集朋友的生日信息（情境相关）相比，采集其教育背景信息（情境无关）的关联隐私关注会增加，但增加的程度目前未见研究报道。

2 文献综述

2.1 隐私价值计量方面

隐私价值计量常常采用隐私成本效益权衡理论。该理论视隐私为一种经济商品，当面临信息披露时，用户有意识地进行成本效益分析，在感知成本和感知收益之间权衡，做出最有利的选择，该过程中用户也会考虑其他因素，比如对信息接收者的信任等。

隐私计量方法常使用实验经济学方法，主要有直接调查法、BDM 实验法、情境模拟法、实地实验法、离散选择实验法、联合分析法和条件价值评估法等。比如，S. Schudy 等[3]使用 BDM 机制通过测量分享个人信息所需的最低金额方法估计不同个人信息项目的价值；R. K. Chellappa 等[4]使用情境模拟法调查在线环境下用户对其个人信息的价值认知，进而探讨个性化服务与隐私泄露之间的权衡机理；S. Spiekermann 等[5]通过测量用户为保留 Facebook 上的个人信息而付费的意愿来评估个人信息隐私价值；H. Krasnova 等[6]采用离散选择实验法研究用户使用 Facebook Connect 等单点登录机制时对个人信息泄露的担忧；I. H. Hann 等[7]采用联合分析法探讨网上披露个人信息的成本和收益之间的权衡，测度个人信息的货币价值；V. Benndorf 等[8]使用条件价值法评估用户贡献给社交网络上个人信息隐私的货币价值。

隐私计量结果与用户调查情境设置有关。情境不同，可选择的调查实验方法有所差异，引入各种基于情境的实验是解决个人信息价值测量挑战的常见方式，在实验中用户需做出影响其隐私认知的行为决定。一般而言，消费者愿意购买隐私友好的产品，但有些情境下存在隐私悖论现象，比如在线购物情境中，用户乐意泄露一些敏感信息以换取更好的个性化服务[9]。平均而言，用户出售个人信息的意愿要高于保护个人信息的意愿，但也有一些情境产生不同的结论，比如医院患者用户非常重视保护敏感度较高的医疗病种数据（如传染病数据），甚至几乎没有出售意愿（如艾滋病数据）。地域和金钱诱导等情境也会影响隐私计量，前者如欧盟各不同国家中个人对其位置数据的货币价值评估的差异，后者如适度的金钱诱惑会导致许多用户贡献其个人信息[10]。隐私政策声明和网络平台的美誉度也是重要的情境变量，比如，J. Kim 等[11]研究发现隐

臧国全，周晓倩. 社交网络中关联隐私的价值计量与分析[J]. 图书情报工作,2020,64(14):85－93.

私声明的存在会对人们披露个人信息的意愿产生正向影响,E. B. Andrade 等[12]调查发现平台声誉与个人隐私关注呈负相关。

2.2 关联隐私方面

在关联隐私产生调查方面,已有一些调查根据社交网络中 APP 下载次数,总结关联隐私的产生情况。比如 2013 年 B. Gergely 等[13]统计 Facebook 中最流行的 2.7 万款 APP 采集朋友信息情况。同年,N. Wang 等[14]调查该社交媒体中使用率最高的 9 400 款 APP 产生关联隐私情况。中国消费者协会[15]分别从 APP Store 和安卓市场下载并测评各 10 类 100 款 APP,发现其中一些要求访问用户朋友信息,比如有 28% 的 APP 要求访问用户的联系人列表(即用户好友),其中一些甚至要求访问用户与其朋友的通话记录。通过分析用户数据也可以得出关联隐私问题的存在,比如,P. Shi 等[16]分析 Facebook 官方博客上发布的用户评论,统计好友信息因用户行为导致泄露所产生的关联隐私关注情况;H. Krasnova 等[6]调查 199 名 Facebook 用户的 38 项朋友信息的隐私关注度,比较用户与朋友的信息收集的关注程度后,发现用户不仅存在“隐私利己主义”现象,也关注朋友信息的泄露。

在关联隐私理论研究方面,至今为止甚少,国内未见报道,国外散见在相关研究中有所涉及,比如,M. E. Johnson[17]依据对企业员工、客户、代理商和供应商的负面影响,分析计算企业对不同类型行为主体信息的被泄露所产生的隐私忧虑。T. L. James 等[18]将用户及知晓其就医敏感数据的朋友视为信息的原始所有者和共同所有者,该就医数据的泄露不仅给原始所有者带来负面影响,也会使共同所有者对原始所有者产生隐私关注,并开发量表进行计量。J. Wirth 等[19]研究个体隐私被泄漏引起知晓其隐私信息的朋友的担忧,并分析后者保护前者隐私动机的影响因素。

3 研究假设与实验情境设置

大量实验研究表明[20－21],许多决策情况下,个体偏离纯粹的自我利益,表现出对他人的偏好,无私关心他人的福祉并回报他人的善意,当个人选择可以直接决定他人利益时,这种偏好表现得尤其强烈。应用到本研究环境,可以预测社交 APP 用户会表现出涉他偏好,关心其朋友的隐私。

还有研究表明[22],基于网络的人际交互可以帮助个人开发和维持在线社会资本。社会资本指通过人际关系积累的非物质资源,有助于个人收获利益,增加不同思想的接触机会和积极价值信息的获取机会。作为在线社区的组成部分,社交 APP 用户或多或少积累在线社交资本,为了维持社会资本产生的积极效益,需评估可能伤害包括好友在内的社区其他成员的行为,比如导致好友信息泄露的行为。因此,可以提出下述假设:

H1:社交 APP 用户正面评价朋友信息的价值,在关联隐私泄露决策情境中存在涉他偏好。

一方面,任何用户(包括 APP 用户)在披露个人信息时,都会表现出隐私担忧,存在涉己偏好[22]。另一方面,APP 用户重视朋友信息,存在涉他偏好,但重视程度会因人和情境不同而有所差异[23]。因此,用户对自己隐私的关注程度是否大于对其朋友隐私的关注程度与情境有关,这是一个实证问题。

但是,人与人之间的联系有强有弱,相互信任以及交际圈紧密重叠的人之间产生较强联系,基于网络互动建立在线社会资本时,用户之间的联系耦合度相对较弱[24]。一般来讲,联系程度越高的人之间的关注程度也越高。因此,可以提出下述假设:

H2:社交用户选择使用 APP 时,对自己信息的隐私关注度高于对其朋友信息的隐私关注度。

情境依赖性指信息收集的合理性依赖于特定情境。在一个特定情境中,若信息收集与情境无关,用户的隐私关注会上升。比如,人们一般不会关注向一个生日 APP 贡献朋友的生日信息,但当 APP 采集与其使用目的无关的信息时,用户的隐私关注会上升[25]。本研究中,数据采集分两种情境:APP 采集用户朋友的信息具有情境依赖性(指 APP 采集的用户朋友信息会提升 APP 的功能实现和使用效果)和不具有情境依赖性(指 APP 采集的用户朋友信息不会提升 APP 的功能实现和使用效果),并提出下述假设:

H3:与社交 APP 采集用户朋友的情境依赖性信息相比,用户对采集其朋友的情境无依赖性信息所产生的关联隐私关注度更高。

基于 H3,本研究实验设置下述两个情境,实验对象被随机分配到其中一个情境,且两个情境的实验对象无交叉。

S1:APP 采集的用户朋友信息不会提升 APP 的功能实现和使用效果。

S2:APP 采集的用户朋友信息会提升 APP 的功能实现和使用效果。

4 研究方案

4.1 联合分析设计

本研究采用联合分析法。该方法由 P. E. Green

等[26]于 1990 年首次提出，用于在成本收益权衡的情境中测量用户偏好，随后被用于估计个人隐私关注的货币价值。本研究中，使用该方法定量估计关联隐私的价值。

联合分析法是一种实验方法，旨在揭示人们选择不同产品的权衡行为。使用该方法，消费者将产品视为多个轮廓，研究人员测试个体对不同轮廓的偏好，每个轮廓由不同属性及其不同水平组成。通过对偏好的统计分析，可以量化每个属性水平的价值，进而推理每个属性水平对个体决策的作用权值。

本研究中，社交 APP 被视为多个属性的组合，采集用户朋友信息是其中一个属性，对应的水平是采集朋友信息的不同类型，通过分析用户评价 APP 的行为，推理用户选择 APP 的影响因素。

4.1.1 属性的确定

采用焦点小组访谈方式，确定联合分析中的社交 APP 属性。访谈的问题是“影响你选择下载使用 APP 的因素有哪些?”

访谈对象共 20 人，均来自郑州大学，其中教师、博士生、硕士生、本科生各 5 人。一半有隐私泄露的经历，另一半则无此类经历，因为该因素可能会影响用户的隐私关注程度。总结访谈结果中主要因素如表 3 所示：

表 3 APP 属性确定的用户访谈结果

人数	因素	典型回答	理论支持或已有研究支持
17	价格	我更倾向于免费 APP，但若对我很重要，我愿意支付少量费用	经济学中的理性人假设
15	受欢迎程度	我更愿意尝试身边朋友使用的 APP	网络人气是人们选择 APP 的重要驱动[27]
14	个人信息的 APP 采集程度	①若 APP 试图收集我的手机号码，我不会考虑这款 APP。②我总是在社交网站上发布虚假信息，这样当我安装该社交网络 APP 时，就无法访问我的真实信息	涉己偏好，即人们通常对个人隐私表现出较高程度的关注[22]
14	朋友信息的 APP 采集程度	他们是我的朋友，我也应该关心他们的隐私	涉他偏好理论[23]

因此，选择使用 APP 的因素主要有 4 个维度：价格、受欢迎程度、用户个人隐私的关注、用户朋友隐私的关注。

4.1.2 水平的确定

在焦点小组访谈中，根据用户选择的属性，进一步进行半结构访谈，获得用户对选择属性的水平认知。

(1) APP 价格的水平。统计苹果应用商店中受欢迎程度排名前 1 000 名的付费 APP 的价格分布，取其平均数。并结合受访者愿意支付的费用情况，选择价格水平为“0 元”和“15 元”。

(2) 受欢迎程度的水平。基于受访者对朋友使用 APP 的比例(即受访者的朋友圈中使用该 APP 的朋友占朋友总数的百分比)进行水平确定。七成受访者认为有三分之一的朋友使用的 APP 即为较受欢迎的 APP，而 10% 以下朋友使用的 APP 可认为较不受欢迎。故将受欢迎程度分为两个水平：10% 和 30%。

(3) 用户个人隐私的水平。基于国家通信行业标准《电信和互联网用户个人信息保护定义和分类》(YD/S2781 -2014)，结合作者对 Facebook 的调查以及手机 APP 应用权限管理功能中 APP 收集个人信息类型，设计 3 个水平：无、基本信息(姓名、证件号码、年龄、性别、工作单位、教育背景、地址等)、完整信息(除基本信息外，还包括定位信息、日程、照片、音频、视频、银行账户等)。

(4) 用户朋友隐私的水平。同用户个人隐私水平。总结 APP 属性及其水平设置如表 4 所示：

表 4 APP 的属性和水平

属性	属性描述	水平
价格	APP 价格	0 元
		15 元
受欢迎程度	用户朋友安装该款 APP 的比例	10%
		30%
用户个人信息	该款 APP 采集用户本人的信息	无
		基本信息
		完整信息
用户朋友信息	该款 APP 采集用户朋友的信息	无
		基本信息
		完整信息

4.1.3 APP 产品轮廓选择

基于表 4，APP 产品轮廓由 4 个属性组成，其中前两个属性各有 2 个水平，后两个属性各有 3 个水平，轮廓总数为 36 个(2×2×3×3)。然而，将 36 个 APP 产品轮廓进行排序是不切实际的，因为参加排序的产品轮廓太多会增加受访者准确排序的难度。为此，使用 SPSS23.0 中正交设计方法，选择代表性轮廓 9 个，见表 5。

4.2 调查设计

采用基于组间设计的在线问卷调查方法，根据研究目的，使用在线调查问卷设计软件“问卷星”设计调查问卷：

臧国全,周晓倩.社交网络中关联隐私的价值计量与分析[J].图书情报工作,2020,64(14):85-93.

(1)问卷测试。测试人员来自郑州大学教师、博士生、硕士生和本科生各5名,评估问卷设计的合理性和内容的正确性。

表5　代表性APP轮廓

编号	价格(元)	受欢迎程度(%)	用户个人信息	用户朋友信息
1	0	10	无	基本信息
2	0	10	基本信息	完整信息
3	0	30	完整信息	无
4	15	10	完整信息	基本信息
5	0	30	基本信息	基本信息
6	0	10	无	无
7	15	10	基本信息	无
8	15	30	无	完整信息
9	0	10	完整信息	完整信息

(2)调查实施。调研团队10人,调研时间为2019年9月至10月,采用滚雪球方式,在郑州大学选取部分师生进行调查,同时邀请他们对身边亲朋好友发放调查问卷。共回收问卷353份。受访者需在至少一个社交网络中拥有账户且安装使用至少10个APP,确保受访者具有社交APP使用经历以保证调查结果质量,有效完成者给予10元奖励。

(3)调查过程。一是简单说明调查目的;二是调查人口统计信息,如性别、年龄、教育程度和职业等;三是排序9个APP轮廓,并配置APP属性和水平的说明供调查对象参考,该部分根据两种情境S1和S2分别调查;四是附加调查,如受访者使用的社交网络中好友数量,进一步分析调查对象的隐私偏好和APP使用行为。

5　数据分析

5.1　样本获取

数据收集阶段共收集353个用户数据,其中S1为175个用户,S2为178个用户。通过数据清洗,筛选掉违反基本常识的低质量问卷。例如,两个轮廓A和B,受欢迎程度相同,收集朋友信息相同,但价格不同(A为15元,B为免费),收集用户信息不同(A采集用户完整信息,B不采集用户信息),理性用户会更喜欢B,如果排名结果相反,则该用户提交结果异常,直接排除。剩余有效问卷S1为103份,S2为102份。

5.2　成分效用值和重要性分析

运行SPSS软件中的联合分析模块,输入问卷调查结果,即可输出联合分析结果指标值,其中包括各属性级别的效用值(见表6)及相对重要性(见表7)。效用值反映用户对某一属性水平的偏好程度,相对重要性反映各属性对于用户选择APP的影响权重。

表6　成分效用值

属性	价格		受欢迎程度		个人隐私			朋友隐私		
水平	0元	15元	10%	30%	无	基本信息	完整信息	无	基本信息	完整信息
S1	1.875	-1.875	-0.383	0.383	1.073	0.206	-1.279	0.565	0.452	-1.017
S2	1.912	-1.912	-0.517	0.517	0.912	0.199	-1.111	0.408	0.320	-0.729

表7　相对重要性

属性	重要性	
	S1(%)	S2(%)
价格	40.225	41.959
受欢迎程度	10.360	12.762
个人隐私	28.226	27.557
朋友隐私	21.189	17.722

由表5和表6可知:价格是用户选择APP时最重要的因素,且当APP价格上升时,效用值下降;个人隐私在两种情境中均排名第二位,且APP收集用户信息越少,效用值越高;朋友隐私位列第三位,当APP收集朋友信息越多时,效用值越低,表明用户选择使用APP时,会考虑朋友隐私,符合隐私决策中的涉他偏好理论;同时,个人隐私的重要性高于朋友隐私,表明用户对个人隐私的关注度高于朋友隐私,符合隐私决策中的涉己偏好理论;受欢迎程度是最不重要因素,且随着受欢迎程度的提高,效用值增加。

5.3　水平变化的货币价值分析

针对一个属性,水平值从一个等级变化到另一个等级时,首先计算用户效用变化(指整体实验对象在一种情境中的平均效用变化);然后计算每一变化的等值货币,反映用户对该变化产生的经济价值认知。计算结果见表8。

表8中,"效用变化"列展示属性的水平变化导致的相应效用变化。两种情境中,APP价格的水平变化导致效用变化最大,表明用户对APP从免费版本变为付费版本时反感程度最大;其次是个人信息,随着APP采集该类信息的水平增加,效用值逐渐变小,效用变化为负值,表明用户更偏向采用收集个人信息更少的APP版本;再次是朋友信息。但受欢迎程度与效用呈现正向关系。

表 8 等级变化导致的效用和货币价值变化

属性	水平变化	效用变化		货币价值		P 值	
		S1	S2	S1	S2	S1	S2
价格	0→15	-3.73	-3.82	-15.00	-15.00	\	\
受欢迎程度	10%→30%	0.77	1.03	3.08	4.04	\	\
个人信息	无→基本信息	-0.87	-0.71	-3.48	-2.79	0.00	0.00
	基本信息→完整信息	-1.48	-1.31	-5.92	-5.14	0.00	0.00
	无→完整信息	-2.35	-2.02	-9.40	-7.93	0.00	0.00
朋友信息	无→基本信息	-0.11	-0.09	-0.44	-0.35	0.13	0.17
	基本信息→完整信息	-1.47	-1.05	-5.88	-4.12	0.00	0.00
	无→完整信息	-1.58	-1.14	-6.32	-4.47	0.00	0.00

效用变化转换为货币价值的算法：首先计算单位价格变化的效用变化值，S1 情境中为 3.73/15 = 0.248 7，S2 情境中为 3.82/15 = 0.254 7；其次计算其他属性水平变化的货币价值，算法是效用变化值除以单位价格变化的效用变化值。例如，朋友信息属性，从采集基本信息到不采集信息，S1 情境下计算货币价值为0.44元，S2 情境下为 0.35，意味着 S1 情境中用户愿意支付 0.44 元以阻止一个 APP 收集朋友的基本信息，而 S2 中愿意为其支付 0.35 元。总体上，用户对于完全阻止 APP 收集朋友信息的货币价值估值 S1 中为 6.32 元，S2 中为 4.47 元。

采用单侧单样本 t 检验，结果显示，除了朋友信息中“无→基本信息”的效用变化不显著外，其他均具显著性。表明用户对朋友基本信息价值的估值很低，但对朋友完整信息价值的估值较高。因此，假设 H1 得到部分支持。

5.4 个人信息的货币价值和朋友信息的货币价值对比

从表 7 中析出个人信息的货币价值和朋友信息的货币价值部分，结果如表 9 所示：

表 9 个人隐私和朋友隐私的货币价值对比

水平变化	S1 中隐私货币价值			S2 中隐私货币价值		
	个人	朋友	P 值	个人	朋友	P 值
无→基本信息	-3.48	-0.44	0.00	-2.79	-0.35	0.00
基本信息→完整信息	-5.92	-5.88	0.04	-5.14	-4.12	0.02
无→完整信息	-9.40	-6.32	0.00	-7.93	-4.47	0.00

由表 9 可知，用户对个人隐私的货币价值估值明显高于对朋友隐私的货币价值估值，说明个体相对于他人更关心自己，符合大众认知。假设 H2 得到支持。

社交网络中，朋友隐私的货币价值意指该用户在该网络中拥有的所有朋友的个人信息估值。举个具体例子，安卓市场中用户下载一个 APP 时，需许可读取通讯录以采集其朋友信息，即产生关联隐私，由于通讯录内含手机用户的所有好友，故关联隐私也为整个好友的隐私。因为用户隐私仅包含一人，为了提高用户隐私与其朋友隐私之间的可比性，需将后者转换为单个朋友的个人信息，转换算法为一位用户的朋友隐私货币价值除以该用户的好友数量，得出一位用户的单个朋友隐私货币价值，再求所有用户的单个朋友隐私值的平均值，结果非常小。因此，用户对其个人隐私估值较高，但对其单个朋友隐私估值非常低，表明用户都是“隐私利己主义者”，网络上大多数朋友的关联耦合度较弱，用户仅关心朋友隐私中很少部分。进一步证实假设 H2 成立。

5.5 两类实验情境中隐私等级变化的货币价值比较

从表 8 中析出实验情境 S1 和 S2 的货币价值部分，结果如表 10 所示：

表 10 不同实验情境中货币价值对比

属性	水平变化	货币价值		P 值
		S1	S2	
个人隐私	无→基本信息	-3.48	-2.79	0.16
	基本信息→完整信息	-5.92	-5.14	0.13
	无→完整信息	-9.40	-7.93	0.01
朋友隐私	无→基本信息	-0.44	-0.35	0.42
	基本信息→完整信息	-5.88	-4.12	0.01
	无→完整信息	-6.32	-4.48	0.01

由表 10 可知，S1 中每一水平变化的货币价值绝对值都高于 S2，表明前者情境中的用户比后者中的更重视隐私，包括用户的个人隐私和朋友隐私。然而，统计分析表明，个人隐私变化在 S1 和 S2 之间均不显著。朋友隐私变化在 S1 和 S2 之间的情况分 3 种：①从“无”到“基本信息”。货币价值差异不显著，说明用户对朋友基本信息关注度低。因此，尽管用户积极评估朋友基本信息，但这种评估不受情境的影响。②从“基本信息”到“完整信息”。相应的 S1 中货币价值显著高于 S2，说明该水平变化伴随着 APP 采集朋友更敏感信息（比如其照片或位置信息）。显著性差异也表明

用户对于朋友有价值的信息比基本信息更敏感。③从“无”到“完整信息”。相应的 S1 和 S2 之间的货币价值变化也存在显著差异,也说明此水平变化包含朋友特别敏感的数据。

上述第一种情况不支持假设 H3,但后两种情况支持假设 H3,即 APP 信息采集环境显著影响用户对朋友特别敏感信息的重视程度,而不是基本信息。因此,假设 H3 得到部分支持。

6 研究结果

本研究提出一种量化关联隐私的货币价值方法。计量 APP 各属性相对重要性,结果显示,两种情境中朋友隐私位列第三,小于用户个人隐私和 APP 价格。比较个人完整信息的货币价值与用户对于其朋友完整信息的货币价值,结果显示,用户选择使用 APP 时会考虑朋友隐私。考虑到朋友数量因素,比较单个朋友的个人信息货币价值与用户个人信息货币价值,前者远远小于后者。上述 3 种情况都表明,用户在决定是否使用 APP 时,同时具有隐私利己属性和隐私利他属性,但前者的程度大于后者。

本研究同时分析社交 APP 采集用户信息的情境对关联隐私价值的影响。S1 情境中用户对个人隐私和对朋友隐私的货币价值估值都高于 S2 情境,但只有当这两种情境作用于朋友的完整信息时产生的关联隐私差异才具有显著性,说明对用户来说,保护基本信息不是那么重要,但对于敏感信息(完整信息中去除基本信息的部分)的不合理请求会对 APP 评价产生负面效用。

7 结语

本研究的理论贡献为:关联隐私问题在国外已得到重视,但在国内少有涉及。关联隐私这一客观现象国内也广泛存在,国内 APP 大多将产生这类隐私的用户朋友信息采集授权以打包方式捆绑在隐私政策中,用户若不同意,则无法继续安装使用。用户朋友往往在不知情的情况下,信息即被泄漏。本研究界定了关联隐私概念,扩充完善了个人隐私的范畴,构建了关联隐私的测度方法。

本研究的实践贡献为:研究结果有助于 APP 隐私政策的制定与完善。用户对朋友信息的估值相对较低,表明此类信息共享应受到更为严格的限制,或让用户好友直接参与决策过程。一方面,隐私政策制定者应鼓励修改完善 APP 隐私声明,明确告知用户 APP 采集其朋友信息的具体操作,包括是否采集朋友信息以及采集朋友信息的类型等。另一方面,应该加强 APP 采集信息的过程管理,比如嵌入一些识别技术,快速判断拟采信息(尤其是朋友的敏感信息)与 APP 功能实现的相关性,以便用户做出有利于保护朋友隐私的决策。因此,从管理和技术角度,采取一些必要干预措施,增加用户乃至其朋友对其相关信息被 APP 采集的知情度,进而提高决策的透明性,是关联隐私管理的可能解决方案。

本研究的局限性表现在:首先,用户使用 APP 的实际决策场景缺少隐私强调机制,但在本研究实验中包括关联隐私在内的隐私问题作为 APP 的两个重要属性直接询问用户的态度认知,可能导致比实际决策情境中更多的隐私关注,隐私货币价值可能被高估,为规避这种可能偏差,已有相关研究在调查中设置不询问用户隐私的情况下测量隐私,未来研究可借鉴此思路。其次,本研究在环境对隐私关注的影响因素设置方面仅考虑 APP 的信息采集环境,即 APP 采集的用户朋友信息是否会提升其功能实现和使用效果,没有纳入其他可能的影响因素,如 APP 的类型和采集信息的具体用途,后续研究需考虑更多维度以更好模拟环境因素与关联隐私价值的关系。最后,本研究虽然证实社交网络中关联隐私的存在,并对其价值给予评估,但并未探讨用户因素的影响,已有研究表明个人经历、信任倾向及人格因素都会影响隐私关注,未来研究可引入结构方程建模讨论这些因素对关联隐私价值的影响。

参考文献:

[1] App Annie:2020 年移动市场报告[EB/OL]. [2020－01－18]. http://www.199it.com/archives/998993.html.

[2] 中华人民共和国国家互联网信息办公室. 百款常用 App 申请收集使用个人信息权限情况[EB/OL]. [2019－08－20]. http://www.cac.gov.cn/2019-05/24/c_1124538535.htm.

[3] SCHUDY S, UTIKAL V. 'You must not know about me'-On the willingness to share personal data [J]. Journal of economic behavior& organization,2017,141(9):1－13.

[4] CHELLAPPA R K, SIN R G. Personalization versus privacy: an empirical examination of the online consumer's dilemma[J]. Information technology & management, 2005, 6(2/3):181－202.

[5] SPIEKERMANN S, BAUER C, KORUNOVSKA J. Psychology of ownership and asset defense: why people value their personal infor-

mation beyond privacy[J]. Social science electronic publishing, 2012, 4(1):41 -47.

[6] KRASNOVA H, ELING N, ABRAMOVA O, et al. Dangers of 'facebook login' for mobile apps: is there a price tag for social information? [EB/OL]. [2019 - 11 - 25]. https://www.researchgate.net/profile/Hanna_Krasnova/publication/277597655_Dangers_of_%27Facebook_Login%27_for_Mobile_Apps_Is_There_a_Price_Tag_for_Social_Information/links/5595030b08ae5d8f392f9584/Dangers-of-Facebook-Login-for-Mobile-Apps-Is-There-a-Price-Tag-for-Social-Information.pdf.

[7] HANN I H, HUI K L, LEE S Y T, et al. Online information privacy: measuring the cost-benefit trade-off[EB/OL]. [2019 -11 -26]. https://aisel.aisnet.org/icis2002/1/.

[8] BENNDORF V, NORMANN H. The willingness to sell personal data[J]. Dice discussion papers, 2018,120(4):1260 - 1278.

[9] SPIEKERMANN S, BERENDT B, GROSSKLAGS J. E-Privacy in 2nd generation E-Commerce: privacy preferences versus actual behavior[EB/OL]. [2019 - 11 - 25]. https://papers.ssrn.com/sol3/papers.cfm? abstract_id =761107.

[10] CHRISTIN N, EGELMAN S, VIDAS T, et al. It's all about the Benjamins: an empirical study on incentivizing users to ignore security advice[C]// Financial cryptography and data security - 15th international conference. Gros Islet:George Danezis,2011:16 -30.

[11] KIM J, NAM C, KIM S. The economic value of personal information and policy implication [C]//26th European regional ITS conference. Madrid: International Telecommunications Society, 2015: 24 -27.

[12] ANDRADE E B, KALTCHEVA V, WEITZ B. Self-disclosure on the web: the impact of privacy policy, reward, and company reputation[J]. Advances in consumer research, 2002, 29(1): 350 - 353.

[13] GERGELY B, CHIA P H. Interdependent privacy: let me share your data[C]// International conference on financial cryptography and data security. Berlin: Springer, 2013:338 -353.

[14] WANG N, GROSSKLAGS J, XU H. An online experiment of privacy authorization dialogues for social applications[C]// Conference on computer supported cooperative work. New York: ACM Press, 2013:261 -272.

[15] 100 款 App 个人信息收集与隐私政策测评报告[EB/OL]. [2019 -08 -28]. http://www.ce.cn/xwzx/gnsz/gdxw/201811/28/t20181128_30892018.shtml.

[16] SHI P, XU H, CHEN Y. Using contextual integrity to examine interpersonal information boundary on social network sites[C]// Sigchi conference on human factors in computing systems. New York: Association for Computing Machinery, 2013:35 -38.

[17] JOHNSON M E. Information risk of inadvertent disclosure: an analysis of file-sharing risk in the financial supply chain[J]. Journal of management information systems,2008,25(2):97 -123.

[18] JAMES T L, WALLACE L, WARKENTIN M, et al. Exposing others' information on online social networks (OSNs): perceived shared risk, its determinants, and its influence on OSN privacy control use[J]. Information & management, 2017, 54(7):851 - 865.

[19] WIRTH J, MAIER C, LAUMER S, et al. Perceived information sensitivity and interdependent privacy protection: a quantitative study[J]. Electronic markets, 2019,29(3):359 -378.

[20] COOPER D, KAGEL J. Other regarding preferences: a selective survey of experimental results[EB/OL]. [2019 - 08 - 25]. https://www.onacademic.com/detail/journal_1000039794745010_ff18.html.

[21] STAHL D O, HARUVY E. Other-regarding preferences: egalitarian warm glow, empathy, and group size[J]. Journal of economic behavior & organization, 2006, 61(1):20 -41.

[22] SMITH H J, BURKE M S J. Information privacy: measuring individuals' concerns about organizational practices[J]. MIS quarterly, 1996, 20(2):167 -196.

[23] FEHR E, RIEDL K A. Does fairness prevent market clearing? an experimental investigation[J]. The quarterly journal of economics, 1993, 108(2):437 -459.

[24] ITOH H. Moral hazard and other-regarding preferences[J]. Japanese economic review, 2004, 55(1):18 -45.

[25] WANG N, WISNIEWSKI P, XU H, et al. Designing the default privacy settings for facebook applications[C]// Proceedings of the companion publication of the 17th ACM conference on computer supported cooperative work & social computing. New York: Association for Computing Machinery, 2014:249 -252.

[26] GREEN P E, SRINIVASAN V. Conjoint analysis in marketing: new developments with implications for research and practice[J]. Journal of marketing, 1990, 54(4):3 -19.

[27] GUPTA S, MELA C F. What is a free customer worth? armchair calculations of nonpaying customers' value can lead to flawed strategies[J]. Harvard business review, 2008, 86(11):102 - 109, 138.

作者贡献说明:

臧国全:提出研究思路,设计研究方案,修订论文;

周晓倩:采集与分析数据,绘制图表,撰写初稿。

臧国全，周晓倩. 社交网络中关联隐私的价值计量与分析[J]. 图书情报工作,2020,64(14):85－93.

Value Measurement and Analysis of Linking Privacy in Social Network

Zang Guoquan[1,2]　Zhou Xiaoqian[1]
[1] School of Information Management, Zhengzhou University, Zhengzhou 450001
[2] Research Institute of Data Science, Zhengzhou University, Zhengzhou 450001

Abstract: [Purpose/significance] With the widespread popularity of social networks, users download a large number of third-party applications (that is, the social APP) through social platforms, which raises privacy concerns. In addition to personal privacy (called direct privacy), the objects of concern also include the privacy of users' friends, called linking privacy. Based on the measurement of the value of linking privacy, the extensive existence of linking privacy is confirmed, which provides a basis for the formulation of linking privacy policy in social apps. [Method/process] Through empirical investigation and literature review, this paper confirmed the extensive existence of linking privacy, and put forward corresponding research questions and research hypotheses. The joint analysis method was adopted to analyze individual preferences through questionnaires, deduced the influencing factors of users' APP selection, and quantitatively estimated the value of related privacy. [Result/conclusion] This paper finds that users consider friends' privacy when they choose to use apps, but value their friends' privacy at a relatively low level. When considering the situation of social APP to collect user information's influence on the linking value of privacy, by introducing two kinds of situations, namely whether the APP to collect user friend information will promote the realization of the function of the APP and use effect, the results show that only when the two kinds of situation on the friend's complete information of linking privacy just have significant differences. It indicates that it is not so important for users to protect the basic information of friends, but unreasonable requests for sensitive information (the part of complete information that removes the basic information) will have a negative effect on APP evaluation.

Keywords: social network　linking privacy　privacy value　privacy measurement